RTCA, Inc.
1150 18th Street NW, Suite 910
Washington, DC 20036
USA

Guidance for Security Event Management

RTCA DO-392
June 23, 2023

Prepared by: SC-216

Copies of this document may be obtained from
RTCA, Inc.
Telephone: 202-833-9339
Facsimile: 202-833-9434
Internet: www.rtca.org
Please visit the RTCA Online Store for document pricing and ordering information.

FOREWORD

This document was prepared by Special Committee 216 (SC-216) Aeronautical Information Systems Security jointly with EUROCAE Working Group 72 (WG-72) and approved by the RTCA Program Management Committee (PMC) and the EUROCAE Council on June 23, 2022.

RTCA, Incorporated is a not-for-profit corporation formed to advance the art and science of aviation and aviation electronic systems for the benefit of the public. The organization functions as a Standards Development Organization and develops consensus-based recommendations on contemporary aviation issues. RTCA's objectives include but are not limited to:

- coalescing aviation system user and provider technical requirements in a manner that helps government and industry meet their mutual objectives and responsibilities;

- analyzing and recommending solutions to the system technical issues that aviation faces as it continues to pursue increased safety, system capacity and efficiency;

- developing consensus on the application of pertinent technology to fulfill user and provider requirements, including development of minimum operational performance standards for electronic systems and equipment that support aviation; and

- assisting in developing the appropriate technical material upon which positions for the International Civil Aviation Organization and the International Telecommunication Union and other appropriate international organizations can be based.

The organization's recommendations are often used as the basis for government and private sector decisions as well as the foundation for many Federal Aviation Administration Technical Standard Orders and advisory circulars.

Since RTCA is not an official agency of the United States Government, its recommendations may not be regarded as statements of official government policy unless so enunciated by the U.S. government organization or agency having statutory jurisdiction over any matters to which the recommendations relate.

DISCLAIMER

This Page Intentionally Left Blank

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 Purpose 1
1.2 Scope 1
1.2.1 Future Aircraft Information Security: Rationale and Needs 2
1.2.2 Treatment of Legacy Aircraft and Systems 4
1.3 How to Use the Document 5
1.4 Conventions of This Document 6
1.5 Relationahip to Other Documents 6

2 INFORMATION SECURITY EVENT MANAGEMENT FRAMEWORK 7

2.1 Introduction 7
2.1.1 Terminology 7
2.1.2 Relationship Between Security Incidents and Security Vulnerabilities 8
2.1.3 Information Security Event Management process 8
2.2 Aviation Stakeholders 10
2.3 Risks Sharing Aspects 11
2.4 Interfacing with Safety Reporting System 11
2.5 Interfacing with IT Security 12
2.6 Documentation and Record Keeping 12

3 ORGANIZE AND PREPARE 15

3.1 Organization & Key People Identification 15
3.2 Information Security Even Management Policy 16
3.3 Security Risk Manageent Contribution for ISEM 17
3.3.1 Introduction 17
3.3.2 Preparation without Security Risk Assessment Inputs for ISEM Process 18
3.3.3 Preparation with Security Risk Assessment Inputs for ISEM Process 19
3.4 Vulnerability Management Consideration 20
3.4.1 Vulnerability Management Overview 20
3.4.2 Vulnerability Management Strategy 21
3.4.3 Vulnerability Disclosure 23
3.5 Information Sharing 24

3.5.1 Purpose 24
3.5.2 Guiding Principles (general) 25
3.5.3 Guiding Principles (technical) 25
3.6 Security Incident Response Team 27
3.6.1 Team Roles and Definitions 27
3.6.2 Capability Building for Security Incident Response Teams 28
3.7 Tooling 28

4 DETECT SECURITY EVENTS 31

4.1 General 31
4.2 Detection Strategy 31
4.2.1 Case 1 – The asset Original Equipment Manufacturer (OEM) has provided guidance or instructions to monitor security during the operation phase. 32
4.2.2 Case 2 - Event detection needs are derived from a security risk assessment 33
4.3 Security Event Information Sources to Monitor 35
4.3.1 System Security Log File Data 36
4.3.2 External Notification 38
4.3.3 Unexplained System Failures (Aircraft and Ground Systems) 38
4.3.4 Physical Evidence of Event 40
4.3.5 Threat Intelligence (Media report, Organizational Feedback…) 41
4.3.6 Vulnerability Monitoring 42
4.4 Recording Events Case Information 42

5 ANALYSE 43

5.1 Introduction on Security Event Analysis 43
5.2 Security Event Triage 44
5.3 Security Incident Analysis 44
5.3.1 Extent of Incident 45
5.3.2 Gather Incident Facts 45
5.3.3 Investigate Log Files 45
5.3.4 Assess Security Incident 46
5.4 Vulnerability analysis 48
5.4.1 Introduction 48
5.4.2 Vulnerability Scoring 49
5.4.3 Vulnerability Triage 49
5.4.4 Vulnerability Risk Assessment 50

5.4.5 Vulnerability Reporting Thresholds 51
5.5 Analysis Time and Emergency Measures 53

6 RESPOND 55

6.1 General 55
6.2 Prioritization 55
6.3 Containment 55
6.4 Tracking and Reporting 56
6.4.1 Notify the Appropriate Individuals 56
6.4.2 Manage Reportable Security Incidents and Vulnerabilities 56
6.4.3 Voluntary Sharing to the Community 58
6.4.4 Report Sequencing 58
6.4.5 Reporting Information Content 59
6.5 Improvements and Lessions Learned 60

7 RECOVER 63

7.1 Introducion 63
7.2 Recovery Planning 63
7.3 React 64
7.3.1 Recovery Action 64
7.3.2 Restoring assets to a safe and secure state 64
7.3.3 Restoring aircraft and associated ground services equipment 65
7.3.4 When to Fail Secure vs. Fail Safe 65
7.3.5 Timeline to Restore 66
7.4 Changes to the Information Security Management System (ISMS) 66
7.5 Recovery Communications 66

APPENDIX A ISEM OBJECTIVES A-1

APPENDIX B VULNERABILITY MANAGEMENT STRATEGY EXAMPLES B-1

APPENDIX C GUIDANCE FOR CVSS SCORING C-1

C.1 Introduction C-1
C.2 Why Use Scoring C-1
C.3 Aviation Guidance for Base Metrics selection C-2
C.4 Aviation Guidance for Temporal Metrics selection C-2

C.5 Aviation Guidance for Environmental Metrics selection C-2
C.5.1 Security Requirements C-3
C.5.2 Modified Exploitability Metrics C-5
C.5.3 Scope C-10
C.5.4 Modified Base Impact Metrics C-11

APPENDIX D GLOSSARY OF TERMS D-1

APPENDIX E ACRONYMS E-1

APPENDIX F REFERENCES F-1

APPENDIX G WG-72 and SC-216 MEMBERSHIP G-1

TABLE OF FIGURES

Figure 2-1: ISEM Process Interfacing Example 9
Figure 2-2: Information Security Even Management Operation Process 10
Figure 3-1 Threat Scenario Visualization 20
Figure 4-1: Asset Event Monitoring Perimeter 33
Figure 4-2: Top-Down Approach to Build the Security Monitoring Perimeter 34
Figure 6-1: Reporting Timeline 58
Figure 7-1: Preparation 68
Figure 7-2: Execution 69
Figure 7-3: Post-Incident 69
Figure C-1: Common Vulnerability Scoring System (CVAA) Metric Groups C-1

TABLE OF TABLES

Table 3-1: Traffic Light Protocol (TLP) Description 26
Table 5-1: Reportability Thresholds 52

1 INTRODUCTION

This document provides guidance on security event management for various stakeholders in the aviation environment such as manufacturers, operators, maintainers, product suppliers, service providers, etc., to develop processes and procedures for identifying, responding to and reporting information security events impacting aviation safety. The guidelines in this document were developed with the intent to provide Acceptable Means of Compliance to EASA's proposed Part IS which intends to establish a regulation requiring approved organizations to implement an Information Security Management System including (Security) Occurrence Reporting analogous to Safety Management System with (Safety) Occurrence Reporting. Other regulations may also apply. Organizations may elect to apply Information Security Event Management processes for operational or other business needs.

Information Security Event Management addresses security events with actual or potential safety consequences. Security events could be malicious interactions (hacking), non-targeted attacks (malware), as well as flaws (vulnerabilities) in systems, components or procedures that could be exploited to cause safety consequences for the aircraft, its passengers or crew.

1.1 Purpose

This document is a resource for civil aviation authorities, government agencies (when applicable), and the aviation industry that need to address information security threats that can affect aviation safety. It addresses the management of security events that affect aviation safety and it supports the existing safety event management guidance. It provides guidance for detection, assessment and disposition, sharing information, reporting and other activities that need to be performed in response to information security events.

Aircraft manufacturers, operators, aviation service providers, maintenance repair and overhaul organizations (MRO), design, manufacturing, operation and regular maintenance of ground ATM/ANS equipment, industrial equipment manufacturing or supporting the production of aircraft and supporting systems and operators of information systems used for support of these functions and all other stakeholders of civil aviation can use this document for event management guidance.

This document is also intended to be a companion to other documents produced by EUROCAE WG-72 and RTCA SC-216 relating to Aeronautical Information System Security. This document is specifically intended for managing information security events that affect aviation safety but is also without prejudice as to its use in other contexts. It is intended to be used along with the safety event management processes defined by 14 CFR 21.3 (FAA), 14 CFR 135.415, 14 CFR 145.221 and Part 21.A.3A (EASA).

Regulatory agencies can publish additional guidance as well as point to existing industry standards, which may be used in combination with this document. Since aircraft information security requirements and regulations evolve, it is recommended that applicants monitor the applicable certification authority’s guidance.

1.2 Scope

This document provides guidance to the aviation sector for the management of information security events with actual or potential aviation safety consequences. This includes unwanted or unexpected events that are an indication of an actual adverse effect on

